**Bezpečnost informací na internetu**

Bezpečnost internetu a bezpečnost práce na internetu se stává stále sledovanější oblastí počítačových sítí a návazných systémů. Internet je bezesporu nevyčerpatelným zdrojem informací. Je to ale také do určité míry nebezpečné médium, kterým se šíří počítačové viry a další nebezpečný a škodlivý počítačový kód

Pocit anonymity na internetu je věc zdánlivá – vyplývá hlavně z neinformovanosti uživatele. Používáním internetových služeb za sebou zanecháváte stopy své činnosti, ať chcete, nebo ne. Tyto stopy lze do jisté míry maskovat, a ztížit tak vaše vystopování. Zjistit lze IP adresu vašeho počítače, operační systém, verzi internetového prohlížeče, typ emailového programu, rozlišení obrazovky a barevnou hloubku. Váš počítač na sebe prozrazuje různé informace v závislosti na systému, který používáte. Vyzrazené informace lze využít a občas i zneužít. Připojení k internetu bez registrace je sice možné, ale neznamená to, že je beze stop k vám.

Hypotetickou cestou jak se nebezpečí vyhnout by bylo odpojit počítač od internetu, či stav, kdy bychom počítač vůbec nezapínali. To je jediná skutečně spolehlivá cesta, jak zabránit útokům a dosáhnout 100% spolehlivosti. Odpojení od internetu a odstavením počítače úplným vypnutím ovšem není řešení, počítač by se tím stal de facto nepoužitelným.

Anonymita na internetu by neměla být vaší prioritou, tou by měla být vaše bezpečnost, tedy zabezpečení vašeho PC a dat na něm uložených. Pokud neděláte nezákonnou činnost, může vám být vaše „neannonymita“ do jisté míry lhostejná.

Je také potřeba vědět, že stát do jisté míry reguluje povinnosti a závazky těch, kdo šíří informace elektronickou formou. Existuje zákon č. 480/2004 Sb., o některých službách informační společnosti, který upravuje odpovědnost, práva a povinnosti osob, jež poskytují služby informační společnosti a šíří obchodní sdělení.

K bezpečnosti informací na internetu patří také zabezpečení emailové schránky proti možnému spamu. Spam patří rovnou do koše, v žádném případě neklepejte na odkazy v něm uvedené.

**Úkol: definuj slovo Spam**

Nebezpečí může přijít i v jiné podobě. V příloze emailu může být uložen jakýkoli soubor – tedy i nebezpečný vir či škodlivý kód. Tento vir vám může přijít i ze známé adresy – třeba od kamaráda, často jako počítačový řetězec. Obranou proti virům je antivirový program. Ten by měl být dostatečně aktuální. Antivirové programy si denně stahují aktualizace od svých výrobců. V každém případě je potřeba si dávat pozor na podezřelou poštu (neznámý odesílatel, příloha, kterou jste nečekali, email v cizím jazyce….) Adresu lze však také podvrhnout – pošta nemusí vždy pocházet od osoby, která je uvedena jako odesílatel.

Všechny tyto viry a další podobná počítačová „havěť“ pochází od počítačově dosti zdatných lidí (zruční programátoři mající znalosti z IT oblasti), jejichž primární „zábavou“ je ovšem nabourávání cizích počítačových systémů a pronikání do nich. Správně se nazývají cracker, mediálně někdy nesprávně označovaní jako hacker.

**Úkol: vysvětli rozdíl mezi hackerem a crackerem**

Dalším nebezpečím spojeným s internetovým světem jsou hoaxy. Pokud těmto zprávám člověk slepě důvěřuje, může udělat více škody než užitku. Jestliže zpráva obsahuje výzvu k rozeslání na další adresy, již to je podezřelé a s největší pravděpodobností se jedná a hoax.

**Úkol: definuj termín Hoax**

Základní zásady bezpečnosti na internetu:

* používej antivirový program – je třeba jej nainstalovat a pravidelně aktualizovat
* udržuj aktuální systém Windows – nastav si automatické aktualizace systému
* neotvírej neznámé či podezřelé soubory (programy či přílohy poštovních zpráv)
* pravidelně zálohuj svá data
* používej bezpečná hesla (velká, malá písmena, čísla i další znaky a alespoň 9 míst)

**Nebezpečí sociálních sítí**

Internet je naším každodenním přítelem a společníkem, ale určitě vás nepřekvapí, že je také nebezpečný. Nebezpečí internetu představuje především volné a nechráněné šíření osobních informací, zvláště pokud nevíte, kam se tato vaše data mohou dostat a kdo je může zneužít.

Toto nebezpečí si však stále mnoho uživatelů neuvědomuje. Pokud využíváte některou sociální síť čistě ke komunikaci se svými přáteli, určitě se nebojíte nahrávat fotky z dovolených a různých party. Občas se stane, že je na fotce něco, co se vám až tak úplně nelíbí, ale přátele tím pobavíte. Co se však stane, když na tyto fotky narazí někdo z vašich budoucích zaměstnavatelů? Co se může stát, když zveřejníte vaši domácí adresu, telefonní číslo či email?

Na těchto sítích se mohou pohybovat různé osoby. Založit si profil je velmi jednoduché a nikdo nekontroluje, zda ten člověk o sobě píše pravdu. Může se tak stát, že sdělujete informace někomu, komu ani nechcete.

Další potencionální nepříjemností může být, že archivy soukromých údajů zvyšují riziko, že budou uživatelé dostávat obtěžující zprávy nebo je někdo osloví se záměrem sexuálního obtěžování apod.

**Úkol: vysvětli termíny Nickname, phishing**

**Úkol: Najdi „Etiketu pro uživatele internetu z roku 1995“ (tzv. Netiketu), napište, kdo je autorem, a vypište sedm pro vás důležitých pravidel chování na internetu**